AMENDMENTS TO THE CLAIMS

Upon entry of the present amendment, the status of the claims will be as is shown below. This listing of claims will replace all prior versions and listings of claims in the application.

1-23. (Canceled)

24. (New) A method for providing a virtual private network, by receiving from a customer originating device of a first local area network, a local area network frame for transmission to a customer destination device in a second local area network over broadband access links that include customer local area network edge devices of at least one customer and an ingress edge device and an egress edge device of a service provider network, the method comprising:

assigning to each edge device of the service provider a unicast IPv6 address, from an IPv6 address block of the service provider, that corresponds to a particular local area network of the customer;

assigning to each edge device of the service provider a virtual private network specific multicast IPv6 address, from the IPv6 address block of the service provider, using the virtual private network specific multicasting IPv6 address for multicasting packets to all of the edge devices of the service provider serving the virtual private network;

determining whether an IPv6 packet includes a destination address of a customer destination device, and whether the destination address is mapped to an egress edge device of the service provider,

when mapping of the destination address to an egress edge device does not exist, encapsulating the local area network frame in a multicast IPv6 packet, the multicast IPv6 packet including the IPv6 address of the ingress edge device of the service provider as the source address and the multicast IPv6 address of the virtual private network as the destination multicast address;

when mapping of the destination address to an egress edge device does exist, encapsulating the local area network frame in a unicast IPv6 packet, including the unicast IPv6 address of the egress edge device of the service provider;

adding a virtual private network identification header to a header of the IPv6 packet, the virtual private network identification header including a destination option, a virtual private network hop count and an identification number identifying the virtual private network of the customer;

broadcasting the IPv6 packets having multicast addresses through the service provider network to all of the edge devices serving the virtual private network;

transmitting the IPv6 packets having the unicast IPv6 address, through the service provider network to a particular egress device;

authenticating the IPv6 packets at the egress device of the service provider using the virtual private network identification;

discarding any IPv6 packets that cannot be authenticated;

decapsulating and extracting the local area network frame of authenticated IPv6 packets at the egress device of the service provider;

forwarding the decapsulated local area network frame to the destination local area network; and

transmitting the decapsulated customer local area network frame to the customer destination device.

25. (New) The method according to claim 24 wherein the ingress edge device of the service provider adds the virtual private network identification number to the IPv6 packet header.

26. (New) The method according to claim 24 wherein the customer local area network edge device adds the virtual private network identification number to the IPv6 packet header, and the ingress edge device confirms the virtual private network identification number.

27. (New) The method according to claim 24, in which the IPv6 packet is discarded when the egress edge device does not recognize the destination option type in the header.

28. (New) The method according to claim 24, in which the virtual private network hop number is incremented every time the IPv6 packet is forwarded by an edge device of the service provider network.

29. (New) The method according to claim 24, in which the egress edge device includes a virtual learning bridge for authenticating the IPv6 packet, the egress edge device determines whether the virtual private network identification number of the received IPv6 packet matches the assigned customer virtual private network identification number, and any IPv6 packets that do not include a matching virtual private network identification number are discarded.

30. (New) The method according to claim 24, in which destination local area network edge device of the customer determines whether the virtual private network identification number of the received IPv6 packet matches the assigned virtual private network identification number and discards unauthorized packets.

31. (New) The method according to claim 24, wherein the authentication of the virtual private network identification numbers can be disabled in the service provider network or the destination local area network to enable interworking among a plurality of virtual private networks.

32. (New) The method according to claim 24, in which the egress edge device includes a virtual learning bridge for learning and caching a mapping of identification information, including an Ethernet MAC address or an identification number of the originating customer device, to the IPv6 address of the ingress edge device, from which the local area network frame was sent, such that when the egress edge device receives subsequent local area network frames

from the customer destination device destined for the customer originating device, the egress edge device encapsulates the local area network frame in a unicast IPv6 packet and unicasts the IPv6 packet to the ingress edge device using the cached mapping.

33. (New) The method according to claim 24, in which edge devices of the service provider are configured to recognize and authenticate multiple, previously assigned virtual private network identification numbers, corresponding to interworking virtual private networks, instead of a single virtual private network identification number corresponding to one customer.

34. (New) A service provider network for providing a virtual private network, for receiving from a customer originating device of a first local area network, a local area network frame for transmission to a customer destination device in a second local area network over broadband access links that include local area network edge devices of the customer coupled to the service provider network, the service provider network comprising:

a plurality of ingress edge devices and egress edge devices;

each edge device being assigned a unicast IPv6 address, from an IPv6 address block of the service provider, that corresponds to a particular local area network of the customer;

each edge device also being assigned a virtual private network specific multicast IPv6 address, from the IPv6 address block of the service provider, which is used for

multicasting packets to all of the edge devices of the service provider serving the virtual private network;

each edge device determining whether an IPv6 packet includes a destination address of a customer destination device, and whether the destination address is mapped to an egress edge device of the service provider,

when mapping of the destination address to an egress edge device does not exist, encapsulating the local area network frame in a multicast IPv6 packet, the multicast IPv6 packet including the IPv6 address of the ingress edge device of the service provider as the source address and the multicast IPv6 address of the virtual private network as the destination multicast address;

when mapping of the destination address to an egress edge device does exist, encapsulating the local area network frame in a unicast IPv6 packet, including the unicast IPv6 address of the egress edge device of the service provider;

wherein a virtual private network identification header is added to a header of the IPv6 packet, the virtual private network identification header including a destination option, a virtual private network hop count and an identification number identifying the virtual private network of the customer;

wherein the IPv6 packets having multicast addresses are broadcast through the service provider network to all of the edge devices serving the virtual private network;

wherein the IPv6 packets having the unicast IPv6 address are transmitted through the service provider network to a particular egress device;

wherein the IPv6 packets are authenticated at the egress devices of the service provider;

wherein any IPv6 packets that cannot be authenticated are discarded;

wherein the local area network frame of authenticated IPv6 packets are decapsulated and extracted at the egress device of the service provider;

wherein the decapsulated local area network frames are forwared to the destination local area network; and

wherein the decapsulated local area network frames are transmitted to the customer destination device.

35. (New) The network according to claim 34 wherein the ingress edge device of the service provider adds the virtual private network identification number to the IPv6 packet header.

36. (New) The network according to claim 34 wherein the customer edge device adds the virtual private network identification number to the IPv6 packet header, and the ingress edge device confirms the virtual private network identification number.

37. (New) The network according to claim 34, in which the IPv6 packet is discarded when the egress edge device does not recognize the destination option type in the header.

38. (New) The network according to claim 34, in which the virtual private network hop number is incremented every time the IPv6 packet is forwarded by an edge device of the service provider network.

39. (New) The network according to claim 34, in which the egress edge device includes a virtual learning bridge for authenticating the IPv6 packet, the egress edge device determines whether the virtual private network identification number of the received IPv6 packet matches the assigned customer virtual private network identification number, and any IPv6 packets that do not include a matching virtual private network identification number are discarded.

40. (New) The network according to claim 34, in which destination local area network edge device of the customer determines whether the virtual private network identification number of the received IPv6 packet matches the assigned virtual private network identification number and discards unauthorized packets.

41. (New) The network according to claim 34, wherein the authentication of the virtual private network identification numbers can be disabled in the service provider network or the destination local area network to enable interworking among a plurality of virtual private networks.

42. (New) The network according to claim 34, in which the egress edge device includes a virtual learning bridge for learning and caching a mapping of identification information, including an Ethernet MAC address or an identification number of the originating customer device, to the IPv6 address of the ingress edge device, from which the local area network frame was sent, such that when the egress edge device receives subsequent local area network frames from the customer destination device destined for the customer originating device, the egress edge device encapsulates the local area network frame in a unicast IPv6 packet and unicasts the IPv6 packet to the ingress edge device using the cached mapping.

43. (New) The network according to claim 34, in which edge devices of the service provider are configured to recognize and authenticate multiple, previously assigned virtual private network identification numbers, corresponding to interworking virtual private networks, instead of a single virtual private network identification number corresponding to one customer.